JOURNAL OF NUMBER THEORY 6, 128–135 (1974)

The Number of Lattice Points on a Convex Curve

H. P. F. SWINNERTON-DYER*

Trinity College, University of Cambridge, Cambridge, England

Communicated May 27, 1971; with revisions February 28, 1972

If C is a strictly convex plane curve of length l, it has been known for a long time that the number of integer lattice points on C is $O(l^{2/3})$ and the exponent is best possible. In this paper, it is shown that the exponent can be decreased by imposing suitable smoothness conditions on C; in particular, if C has a continuous third derivative with a sensible bound, the best possible value of the exponent lies between 3/5 and 1/3 inclusive.

1. Let C be a strictly convex curve in the (x, y) plane, and assume for convenience that the origin lies inside C. For any $N > 0$, let NC denote the curve obtained from C by N-fold magnification about the origin; thus the point (x, y) is on NC if and only if $(N^{-1}x, N^{-1}y)$ is on C. Denote by $S_N(C)$ the number of integer points on NC. George Andrews has raised the question whether

$$S_N(C) = o(N^\epsilon) \qquad \text{as} \quad N \to \infty \tag{1}$$

holds for every $\epsilon > 0$, either for all C or at least for a restricted class of C. If this were true, and the restriction on C was not too onerous, there would be interesting applications to the theory of arithmetic functions.

More generally, for any strictly convex curve C we can define

$$\sigma(C) = \limsup_{N \to \infty} \left(\frac{\log S_N(C)}{\log N} \right),$$

and we can ask for the least upper bound of $\sigma(C)$ as C runs through a given class of strictly convex curves. When C is unrestricted, this problem has been solved by Jarník [1], who proved

THEOREM 1. *Let C be a strictly convex closed curve of length $l > 3$;*

* Harvard University, Cambridge, Massachusetts, January 1971–January 1972.

then the number of integer points on C does not exceed $3(2\pi)^{-1/3}l^{2/3} + O(l^{1/3})$. *Both the exponent and the constant in the leading term are best possible.*

It follows at once that $\sigma(C) \leqslant 2/3$ for all strictly convex C; and a slight modification of the curve which Jarník constructs to show that Theorem 1 is best possible, will show that this result also is best possible. One is therefore led to consider restricted classes of C, and the natural restriction to impose is differentiability to a higher order. The first object of this paper is to show that no condition weaker than infinitely many times differentiable is adequate to ensure (1). This will be done in §2, by proving

THEOREM 2. *For any integer* $n > 1$ *there is a strictly convex curve* C_n *which is n times continuously differentiable and is such that* $\sigma(C_n) \geqslant n^{-1}$.

This result is probably not best possible for any n, in view of the crudeness of the construction used in the proof. In particular, I conjecture that there exists a twice continuously differentiable curve C_2' such that $\sigma(C_2') = 2/3$, which would be best possible in view of (2), and also that there exists a three times continuously differentiable curve C_3' with $\sigma(C_3') \geqslant 1/2$.

The second object of this paper is to show that differentiability conditions are at any rate relevant to the problem. This will be done in §3, by proving

THEOREM 3. *Let C be a strictly convex curve which is three times continuously differentiable; then* $\sigma(C) \leqslant 3/5$.

As with Theorem 2, the crudeness of the argument makes it very unlikely that this is best possible. The ideas underlying the proof of Theorem 3 can also be applied when C is n times continuously differentiable for some fixed $n > 3$, but as yet I have only been able to obtain in these cases very small improvements on the bound given by Theorem 3.

2. In this section we prove Theorem 2. We shall regard n as a fixed integer; everything in the construction will depend on n, but this dependence will be omitted in order to simplify the notation. The major part of the proof consists of the construction of a sequence of triples $\{\Gamma_\nu, \mathscr{S}_\nu, N_\nu\}$ for $\nu = 1, 2, \ldots$, where Γ_ν is a strictly convex curve, $\mathscr{S}_\nu$ is a finite set of points on Γ_ν and N_ν is a positive integer. Let the equation of Γ_ν in polar coordinates be $r = f_\nu(\theta)$, and write $\phi_\nu(\theta) = f_\nu(\theta) - f_{\nu-1}(\theta)$ whenever $\nu > 1$; note that the radius of curvature at any point of Γ_ν is given by

$$\rho_\nu = (f_\nu^2 + f_\nu'^2)^{3/2}/(f_\nu^2 + 2f_\nu'^2 - f_\nu f_\nu''), \tag{3}$$

where the dashes denote differentiation with respect to θ. The triples will be constructed in such a way as to have the following properties:

(i) each Γ_ν is n times continuously differentiable and $|\phi_\nu^{(m)}| \leqslant 2^{-\nu-1}$ for $m = 0, 1, \ldots, n$, and all θ;

(ii) the set $\mathscr{S}_\nu$ contains at least N_ν^c points, where $c = c_\nu = n^{-1}(1 - \nu^{-1})$;

(iii) if P is any point of $\mathscr{S}_\nu$ then $N_\nu P$ is an integer point;

(iv) N_ν is a proper factor of $N_{\nu+1}$, which implies that $N_\nu \to \infty$;

(v) $\mathscr{S}_\nu \subset \mathscr{S}_{\nu+1}$, so that the sequence of $\mathscr{S}_\nu$ is monotone increasing.

Moreover Γ_1 is the unit circle, $\mathscr{S}_1$ consists of the four points $(\pm 1, 0)$ and $(0, \pm 1)$, and $N_1 = 1$.

Choose once-for-all a real-valued function $g(t)$ defined in $0 \leqslant t \leqslant 2\pi$ which is n times continuously differentiable (one-sidedly at 0 and 2π), strictly positive for $0 < t < 2\pi$ and such that $g(t)$ and its first n derivatives all vanish at $t = 0$ and at $t = 2\pi$. For example we may take $g(t) = \{t(2\pi - t)\}^{n+1}$. Let A_1 and A_2 be constants such that

$$g(t) \geqslant A_1 > 0 \qquad \text{for} \quad |t - \pi| \leqslant 1, \tag{4}$$

$$|g^{(m)}(t)| \leqslant A_2 \qquad \text{for} \quad 0 \leqslant t \leqslant 2\pi \quad \text{and} \quad m = 0, 1, \ldots, n. \tag{5}$$

Now suppose that for some $\mu \geqslant 1$, the first μ triples have already been constructed and satisfy (i) to (v) above; we shall construct the $(\mu + 1)$th triple to satisfy these conditions. It follows from (i) and $f_1(\theta) = 1$ that $5/4 > f_\mu > 3/4$ and $|f_\mu^{(m)}| < 1/4$ for $m = 1, 2, \ldots, n$. Thus a circle of radius N^{-1} whose centre lies on Γ_μ will subtend an angle of at most $4N^{-1}$ at the origin, provided N is large enough; and if (r, θ) is any point of the circle,

$$|r - f_\mu(\theta)| < 2N^{-1}. \tag{6}$$

Write $c = c_{\mu+1} = n^{-1}(1 - (\mu + 1)^{-1})$, which is the exponent in condition (ii), and choose integers M, N such that N_μ is a proper factor of N and

$$M \geqslant N^c, \qquad A_1 N \geqslant 2^{\mu+3} A_2 M^n; \tag{7}$$

we can clearly also assume that N is large enough for (6) to hold and for any circle of radius N^{-1} whose centre lies on Γ_μ to subtend an angle at most $2M^{-1}$ at the origin. $N_{\mu+1}$ will be the N thus chosen.

We must define $\Gamma_{\mu+1}$, which we do by defining $\phi_{\mu+1}$ separately in each of the M sectors

$$2\pi m M^{-1} \leqslant \theta \leqslant 2\pi(m + 1) M^{-1} \tag{8}$$

for $m = 0, 1, \ldots, M-1$. If there is a point of $\mathscr{S}_\mu$ in the interior of the sector (8), then we take $\phi_{\mu+1}(\theta) = 0$ in that sector. If not, let R_m be the circle of radius N^{-1} whose centre is the point of Γ_μ for which $\theta = 2\pi(m + 1/2)\, M^{-1}$, and let P_m be a point in the interior of R_m such that NP_m is an integer point; such a P_m exists since any circle of radius 1 in the plane contains at least one integer point. Now set

$$\phi_{\mu+1}(\theta) = \lambda_m g(M\theta - 2\pi m)$$

in the sector (8), where the constant λ_m is to be chosen so that $\Gamma_{\mu+1}$ goes through P_m. It follows from (4) and (6) that $|\lambda_m| < 2/A_1 N$, and hence condition (i) for $\Gamma_{\mu+1}$ follows from (5) and the second equation (7). Finally, we choose $\mathscr{S}_{\mu+1}$ to be the union of $\mathscr{S}_\mu$ and all the points P_m used in the construction of $\Gamma_{\mu+1}$. Conditions (iii), (iv), and (v) are obviously satisfied, and (ii) follows from the first equation (7) together with the fact that each sector (8) has at least one point of $\mathscr{S}_{\mu+1}$ in its interior.

We have still to show that $\Gamma_{\mu+1}$ is strictly convex. But it now follows from (i) that

$$5/4 > f_{\mu+1} > 3/4, \qquad |f'_{\mu+1}| < 1/4, \qquad |f''_{\mu+1}| < 1/4,$$

and a crude estimate from (3) gives $7 > \rho_{\mu+1} > 1/5$; since $\rho_{\mu+1}$ is strictly positive, $\Gamma_{\mu+1}$ is strictly convex. This completes the construction of the triples.

Now let C_n be the curve $r = f(\theta)$ where

$$f(\theta) = \lim_{\nu\to\infty} f_\nu(\theta) = 1 + \sum_{\mu=2}^{\infty} \phi_\mu(\theta),$$

so that in an obvious sense C_n is the limit of the Γ_ν. It follows from (i) that we can differentiate this series term by term up to n times, and therefore C_n is n times continuously differentiable. The argument which proved that $\Gamma_{\mu+1}$ is strictly convex proves the same for C_n; and by construction C_n contains each $\mathscr{S}_\nu$ so that $\sigma(C_n) \geqslant \limsup c_\nu = n^{-1}$. This completes the proof of Theorem 2.

3. In this section we prove Theorem 3. We retain the definitions and notation of Section 1, but forget those of Section 2. The key to the proof is the following lemma, which is well known in interpolation theory but for which I can give no completely satisfactory reference.

LEMMA 1. *For a given integer $n > 0$ let $x_0 < x_1 < \cdots < x_n$ be $(n+1)$ real numbers and let $f(x)$ be n times differentiable in $x_0 \leqslant x \leqslant x_n$. Let*

$g(x) = a_0x^n + \cdots$ be the unique polynomial of degree n such that $g(x_\nu) = f(x_\nu)$ for $\nu = 0, 1,..., n$. Then there exists ξ such that $x_0 < \xi < x_n$ and $f^{(n)}(\xi) = n!\, a_0$.

Proof. We have $g^{(n)}(\xi) = n!\, a_0$ for any ξ, so by considering $f - g$ instead of f, we can reduce to the special case when every $f(x_\nu) = 0$ and we have to prove $f^{(n)}(\xi) = 0$. By the mean value theorem, there exist $x_0', x_1',..., x_{n-1}'$ such that $x_\nu < x_\nu' < x_{\nu+1}$ (which implies that the x_ν' are all distinct) and $f'(x_\nu') = 0$. Repeating this argument n times, we obtain the special result to which we have reduced the lemma.

For the application it will be convenient to make a change of notation, writing

$$u_\nu = x_\nu - x_{\nu-1}, \qquad v_\nu = f(x_\nu) - f(x_{\nu-1})$$

for $\nu = 1, 2,..., n$. The two cases we shall need are $n = 2$, when the lemma gives

$$1/2f''(\xi) = \frac{u_1v_2 - u_2v_1}{u_1u_2(u_1 + u_2)}, \tag{9}$$

and $n = 3$, when it gives

$$1/6f'''(\xi) = \frac{u_1(u_1 + u_2)(u_2v_3 - u_3v_2) - u_3(u_2 + u_3)(u_1v_2 - u_2v_1)}{u_1u_2u_3(u_1 + u_2)(u_2 + u_3)(u_1 + u_2 + u_3)}. \tag{10}$$

We shall use these equations to provide bounds for the absolute values of the right-hand sides. We shall also need an estimate for $(u_1v_3 - u_3v_1)$. By the mean value theorem, v_1/u_1 is the value of $f'(x)$ at some point x with $x_0 < x < x_1$, and similarly v_3/u_3 is the value of $f'(x)$ at some point x with $x_2 < x < x_3$. These two values of x are at most $(u_1 + u_2 + u_3)$ apart, so

$$|u_1v_3 - u_3v_1| \leqslant u_1u_3(u_1 + u_2 + u_3) \max |f''(\xi)|. \tag{11}$$

Now let C^* be a three times continuously differentiable arc whose equation is $y = f(x)$; and suppose that $|f'| \leqslant 1$ on C^* and that C^* is strictly convex upwards, which implies $f'' \leqslant 0$ with strict inequality almost everywhere. Thus there are constants A_2, A_3 such that

$$0 \geqslant f'' \geqslant -A_2, \qquad |f'''| \leqslant A_3 \tag{12}$$

on C^*. Let α be a real number such that $1/3 < \alpha < 2/5$ and let N be a large positive integer. In what follows, the 'O' notation will refer to estimates as $N \to \infty$ and the implied constant will depend only on A_2, A_3

and α. Let $P_0 = (x_0, y_0),..., P_3 = (x_3, y_3)$ be four points on C^* such that $x_0 < x_1 < x_2 < x_3$ and each NP_ν is an integer point; and write

$$u_\nu = x_\nu - x_{\nu-1}, \qquad U_\nu = Nu_\nu, \qquad v_\nu = y_\nu - y_{\nu-1}, \qquad V_\nu = Nv_\nu.$$

Clearly the U_ν are positive integers and the V_ν are integers with $|V_\nu| \leqslant U_\nu$.

LEMMA 2. *Let $1/3 < \alpha < 2/5$; then with the notation above there are at most $O(N^{9\alpha-3+\epsilon})$ sets of points $P_1,..., P_4$ such that $U_1 + U_2 + U_3 < N^\alpha$, where ϵ is any preassigned positive number.*

Proof. Write

$$\Delta_{21} = U_2V_1 - U_1V_2, \quad \Delta_{32} = U_3V_2 - U_2V_3, \quad \Delta_{31} = U_3V_1 - U_1V_3; \quad (13)$$

then Δ_{21}, Δ_{32}, and Δ_{31} are integers which are strictly positive by the strict convexity of C^*, and they are all $O(N^{3\alpha-1})$ by (9) and (11). Moreover

$$U_2\Delta_{31} = U_1\Delta_{32} + U_3\Delta_{21}. \quad (14)$$

Similarly (10) implies that

$$U_1(U_1 + U_2)\Delta_{32} - U_3(U_2 + U_3)\Delta_{21} = O(N^{6\alpha-2}), \quad (15)$$

and eliminating U_2 from this by means of (14) gives

$$\Delta_{32}(\Delta_{31} + \Delta_{32})U_1^2 - \Delta_{21}(\Delta_{31} + \Delta_{21})U_3^2 = O(N^{6\alpha-2}\Delta_{31}). \quad (16)$$

We now regard Δ_{21}, Δ_{32}, and Δ_{31} as temporarily fixed, and obtain an upper bound for the number of sets U_1, U_2, U_3, V_1, V_2, V_3 satisfying (13), (14), and (16); the first step in this is to find the number of acceptable solutions U_1, U_3 of (16).

Since $\Delta_{21} \geqslant 1$ and $U_1 + U_2 < N^\alpha$, it follows from (9) and (12) that

$$U_\nu > 2A_2^{-1}N^{1-2\alpha} \quad (17)$$

for $\nu = 1$ or 2; and a similar argument works for $\nu = 3$. Without loss of generality we may assume that $\Delta_{21} \geqslant \Delta_{32}$; then (16), (17), and $\alpha < 2/5$ together imply that $U_3 < 2U_1$ provided N is large enough, the bound on N depending only on A_2 and α. (Indeed the sole purpose of the hypothesis $\alpha < 2/5$ is to ensure that each of the two terms on the left of (16) is large compared to their difference.) Now suppose that (U_1', U_3') and (U_1'', U_3'') are two acceptable solutions of (16) which satisfy $2 \geqslant U_1'/U_1'' \geqslant 1/2$. It follows that

$$\Delta_{32}(\Delta_{31} + \Delta_{32})(U_1'^2U_3''^2 - U_1''^2U_3'^2) = O(N^{6\alpha-2}\Delta_{31}(U_3'^2 + U_3''^2)). \quad (18)$$

But $U_3''^2 + U_3''^2 = O(U_1'U_3'' + U_1''U_3')$ by the conditions already imposed; so (18) reduces to

$$U_1'U_3'' - U_1''U_3' = O(N^{6\alpha-2}\Delta_{32}^{-1}). \tag{19}$$

Let U_2', U_2'' be the corresponding values of U_2 derived from (14), which must be integers; then it follows from (14) that

$$\Delta_{32}(U_1'U_3'' - U_1''U_3') = \Delta_{31}(U_2'U_3'' - U_2''U_3'),$$

and hence that $U_1'U_3'' - U_1''U_3'$ is divisible by $\Delta_{31}/(\Delta_{31}, \Delta_{32})$, where the bracket denotes highest common factor. Similarly it is divisible by $\Delta_{31}/(\Delta_{31}, \Delta_{21})$, and hence even by $\Delta_{31}D^{-1}$ where

$$D = (\Delta_{31}, \Delta_{32}, \Delta_{21}). \tag{20}$$

So in virtue of (19) there are at most $O(N^{6\alpha-2}D\Delta_{31}^{-1}\Delta_{32}^{-1})$ possible values of $U_1'U_3'' - U_1''U_3'$.

Now suppose (in addition to all the previous hypotheses) that

$$(U_1', U_3') = d = (U_1'', U_3'')$$

for some assigned d, which must clearly be a factor of Δ_{31}. Then to given values of U_1', U_3' and $U_1'U_3'' - U_1''U_3'$ there are at most two possible pairs U_1'', U_3'' with $2U_1' \geqslant U_1'' > 0$. So to given values of the Δ_{ij} and $d = (U_1, U_3)$, there are at most $O(N^{6\alpha-2}D\Delta_{31}^{-1}\Delta_{32}^{-1})$ acceptable pairs U_1, U_3 with U_1 satisfying $2R \geqslant U_1 \geqslant R$, for any preassigned R; and we can cover the possible range of values of U_1 by means of $O(\log N)$ values of R. Since d is a factor of Δ_{31}, the number of possible values of d is at most the number of factors of Δ_{31}, which is $O(N^{\epsilon})$ for any $\epsilon > 0$ where the implied constant depends on ϵ but not on Δ_{31}. So finally the number of acceptable solutions of (16) is $O(N^{6\alpha-2+\epsilon}D\Delta_{31}^{-1}\Delta_{32}^{-1}\log N)$; and the factor $\log N$ can be absorbed into the term N^{ϵ}.

For given values of U_1 and U_3, U_2 is then uniquely determined by (14) and the V_ν have to be chosen to satisfy (13). They are thus determined up to the possibility of adding λU_ν, where λ is a rational number whose denominator must be a factor of (U_1, U_2, U_3) since the V_ν are integers. Clearly (U_1, U_2, U_3) divides each Δ_{ij} and thus also D; and since we must have $|V_\nu| \leqslant U_\nu$, it follows that for given U_1, U_3 there are at most $O(D)$ acceptable sets of values of U_2, V_1, V_2, V_3. So for fixed Δ_{ij} there are at most $O(N^{6\alpha-2+\epsilon}D^2\Delta_{31}^{-1}\Delta_{32}^{-1})$ sets of values of the U_ν and V_ν.

Now fix D and sum over all the values of the Δ_{ij} subject to (20) and $\Delta_{ij} = O(N^{3\alpha-1})$. We can instead of (20) let the Δ_{ij} run through all strictly positive multiples of D up to the assigned bound because this can only

increase the sum; it follows that there are $O(N^{9\alpha-3+\epsilon}D^{-1}\log^2 N)$ acceptable sets of U_ν and V_ν with the given value of D. Summing over the possible values of D, which are again $O(N^{3\alpha-1})$, produces $O(N^{9\alpha-3+\epsilon}\log^3 N)$; and the $\log^3 N$ can be absorbed into the N^ϵ. This completes the proof of the lemma.

Proof of Theorem 3. Divide C into four arcs, the division points being the points at which $dy/dx = \pm 1$. It is enough to estimate the contribution to $S_N(C)$ from one of these arcs, say from the topmost one. Call this arc C^* and note that it satisfies the conditions imposed on the C^* of Lemma 2. Let $Q_0, \ldots, Q_M$ be the points of C^* such that NQ_m is an integer point; write $Q_m = (x_m, y_m)$ and suppose that the Q_m are arranged in order of increasing x. By Lemma 2 there are at most $O(N^{9\alpha-3+\epsilon})$ values of m such that $x_{3m+3} - x_{3m} < N^{\alpha-1}$; and since $x_M - x_0$ is bounded by the diameter of C, there are at most $O(N^{1-\alpha})$ values of m for which $x_{3m+3} - x_{3m} \geqslant N^{\alpha-1}$. Thus

$$S_N(C) = O(N^{9\alpha-3+\epsilon} + N^{1-\alpha}),$$

and the theorem follows on first taking $\alpha = 2/5 - \epsilon$ and then letting ϵ tend to 0.

REFERENCE

1. V. JARNÍK, Über die Gitterpunkte auf konvexen Kurven, *Math. Zeit.*, **24** (1925), 500–518.